(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002342144 A**

(43) Date of publication of application: **29.11.02**

(51) Int. Cl **G06F 12/00**
G06F 12/14
G06F 15/00

(21) Application number: **2001151188**

(22) Date of filing: **21.05.01**

(71) Applicant: **TOSHIBA CORP**

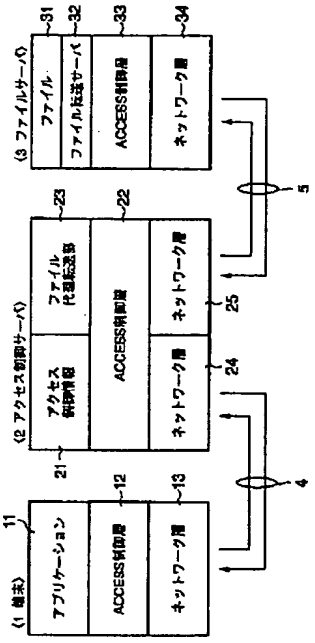
(72) Inventor: **KAWATOU TOSHIYUKI**
TOYODA ISAMU

(54) FILE SHARING SYSTEM, PROGRAM AND FILE TRANSFERRING METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To acquire advanced security.

SOLUTION: In this file sharing system, an access control server 2 is connected between a plurality of terminals 1,... sharing files and a file server 3 storing entity files through respective different networks 4 and 5, a terminal 1 can not access directly to the file server 3, and the access control server 2 judges access request contents from the terminal, and requests a file from the file server 3 to transfer the file to the request source terminal when the access request contents have appropriate authority.



ENGLISH TRANSLATION OF PERTINENT SECTIONS OF JAPANESE LAID-OPEN PATENT PUBLICATION NO.2002-342144 (filed on May 21, 2001)

[Tiltle of the Invention]

File Sharing System and Program, and File Transfer Method

[Means Used to Solve the Problem]

(1) To solve the above problems, a file sharing system according to the present invention in which a plurality of terminals share files using a network includes at least one file server that stores files; and a control server independent from the file server that manages access control information of the files, refers to the access control information based on an access request from one of the terminals, obtains a file from the file server according to a request authorization, and sends the obtained file to the requestor terminal.

According to the present invention having the above configuration, an access control server that manages access control information of files is implemented between the terminals and the file server, and thereby, the access control server may refer to the access control information according to an access request from a terminal, determine whether authorization for the access request is given, and, if the access request is authorized, the access control server may obtain a file from the file server as necessary and transfer the obtained file to the requestor terminal. In this way, flexible access control may be realized.

(2) A file sharing system according to the present invention includes a plurality of terminals that share files; at least one file server that stores the files; an access control server that manages access control information of the files and is connected to the terminals and the file server via differing networks.

According to the present invention having the above configuration, the access control server is connected to the terminals and the file server via differing networks, and the access control server manages the access information of the files. In this way, security in the strict sense of the word may be guaranteed.

(3) A program according to the present invention is run on a computer that receives a file access request from a terminal, requests for a file stored in a file server, and sends the file to the requestor terminal, the program administering the computer to realize: a file/user search function of referring to pre-arranged access control information based on a file name and identification data pertaining to a user that are described in a file access request format that is sent from the terminal, and determining

whether a logical file corresponding to the file name and identification data corresponding to the identification data in the access request format exist; a request type determination function of determining a type of the request described in the access request format when the existence of the logical file and user identification data is verified by the file/user search function; an authorization check function of determining whether the type of request determined by the request type determination function is in agreement with authorization set in the access control information; and a function of coordinating with the file server to execute the type of request when the authorization is recognized by the authorization check function.

According to the present invention having the above configuration, a program for administering a computer to realize the above described functions is provided. Thus, when a file access request is received from a terminal, the computer refers to access control information based on information described in the access request format, searches for the requested file and the pre-registered user information, and when both file and user registration are found, determines the type of request described in the access request format, and whether the user has authorization to make the type of request, and when the authorization is recognized, the computer obtains a file from the file server according to the type of request and sends the file to the requestor terminal. In this way, a substantial file in the file server may be transferred while realizing flexible access control and maintaining high security depending on the definition of the access control information.

(4) A shared file transfer method according to the present invention includes: an access request step of sending an access request according to a predetermined access request format from a terminal; a referring step in which an access control server managing access control information of files refers to the access control information based on a file name and identification data pertaining to a user that are described in a file access request format that is sent from the terminal, and determines whether a logical file corresponding to the file name and identification data corresponding to the identification data in the access request format exist; a request type determination step in which the access control server determines a type of the request described in the access request format when the existence of the logical file and the user identification data is verified in the referring step; an authorization check step in which the access control server refers to the access control information based on the type of request determined in the request type determination step and checks whether the type of request is authorized; and a transfer step in which the access control server sends a file list to the requestor terminal, or requests for a file to the file server and sends the

obtained file to the requestor terminal according to the type of request when authorization for the type of request is recognized in the authorization check step. In this way, a file is obtained from the file server according to the type of request and transferred to the requestor terminal, and thereby, a substantial file in the file server may be transferred to the requestor terminal while realizing flexible access control and maintaining high security.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－342144
（P2002－342144A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
G06F	12/00	537	G06F	12/00	537A	5B017
		545			545A	5B082
	12/14	310		12/14	310K	5B085
	15/00	330		15/00	330A	

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

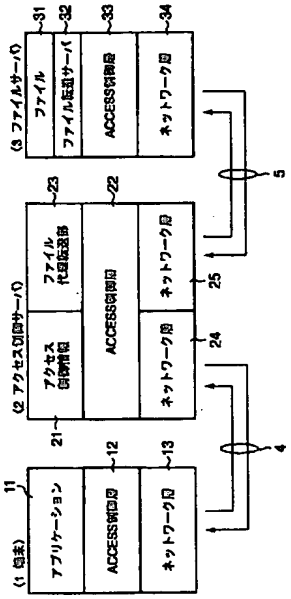
(21)出願番号　特願2001－151188(P2001－151188)
(22)出願日　平成13年５月21日(2001.5.21)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　川嶌　利之
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(72)発明者　豊田　勇
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　ファイル共有システム、プログラムおよびファイル受渡し方法

(57)【要約】
【課題】　高度なセキュリティを確保することにある。
【解決手段】　ファイルを共有する複数の端末１，…と実体のファイルを格納するファイルサーバ３との間にアクセス制御情報を管理するアクセス制御サーバ２がそれぞれ異なるネットワーク４，５で接続し、端末１からファイルサーバ３への直接のアクセスを不可とし、端末からのアクセス要求内容をアクセス制御サーバ２で判断し、適切な権限を有するとき、ファイルサーバ３にファイルを要求し、要求元端末に転送するファイル共有システムである。



1

【特許請求の範囲】

【請求項１】　複数の端末がネットワークを利用してファイルを共有するファイル共有システムにおいて、
前記ファイルを格納する少なくとも１台のファイルサーバと、このファイルサーバから独立して前記ファイルのアクセス制御情報を管理し、前記端末からのアクセス要求に基づいて当該アクセス制御情報を参照し、前記アクセス要求に応じた権限を有するとき、その権限内において前記ファイルサーバからファイルを取得し要求元端末に転送するアクセス制御サーバとを備えたことを特徴とするファイル共有システム。

【請求項２】　ファイルを共有する複数の端末と、前記ファイルを格納する少なくとも１台のファイルサーバと、前記ファイルのアクセス制御情報を管理し、複数の端末と前記少なくとも１台のファイルサーバとに対して、異なるネットワークで接続されているアクセス制御サーバとを備え、
当該アクセス制御サーバが前記各端末から前記ファイルサーバへの直接的なアクセスを制限することを特徴とするファイル共有システム。

【請求項３】　請求項１または請求項２に記載のファイル共有システムにおいて、
前記アクセス制御サーバは、ファイルのアクセス制御情報を管理する手段と、
前記ファイルを共有する各端末からのアクセス要求に基づいて前記アクセス制御情報を参照し権限有無をチェックするアクセス制御手段と、このアクセス制御手段によってファイル転送に関連する権限が有ると判断したとき、前記ファイルサーバにファイルの要求を行い、得られたファイルを要求元端末に転送するファイル代理転送部とを備えたことを特徴とするファイル共有システム。

【請求項４】　各端末からのファイルのアクセス要求を受け、ファイルサーバに格納されるファイルを要求し前記要求元端末に転送するコンピュータに、
前記各端末から送信されてくるファイルのアクセス要求フォーマットに記載するファイル名およびユーザに関連する識別データに基づき、予め管理されているアクセス制御情報を参照し、ファイル名に相当する論理ファイル、前記識別データと同一の識別データが存在するか否かを判断するファイル・ユーザ存在検索機能と、この機能によって存在すると判断されたとき、前記アクセス要求フォーマットに記載する要求種別を判断する要求種別判断機能と、この機能によって判断された要求種別が前記アクセス制御情報に定める権限に合致するか否かを判断する権限チェック機能と、この機能により権限有りと認定されたとき、ファイルサーバと連携し前記要求種別を実現する機能とを実現させるためのプログラム。

【請求項５】　端末からのアクセス要求に応じてファイルサーバに格納されるファイルの受渡しを行う共有ファイル受渡し方法において、

2

各端末から所定のアクセス要求フォーマットに応じたアクセス要求を送出するアクセス要求ステップと、ファイルのアクセス制御情報を管理するアクセス制御サーバが前記各端末から送信されてくるファイルのアクセス要求フォーマットに記載されるファイル名およびユーザに関連する識別データに基づき、前記アクセス制御情報を参照し、ファイル名に相当する論理ファイル、前記識別データと同一の識別データが存在するか否かを検索する検索ステップと、このステップにより存在すると判断されたとき、前記アクセス制御サーバが前記アクセス要求フォーマットに記載する要求種別を判断する要求種別判断ステップと、このステップにより判断された要求種別に基づき、前記アクセス制御サーバが前記アクセス制御情報を参照し、当該要求種別に対する権限有無をチェックする権限チェックステップと、このステップによって権限有りと判断されたとき、前記アクセス制御サーバが前記要求種別に応じてファイルリストを前記要求元端末に転送し、或いは前記ファイルサーバにファイルを要求し、取得されたファイルを前記要求元端末に転送する転送ステップとを有することを特徴とする共有ファイル受渡し方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを利用したファイル共有システム、プログラムおよび共有ファイル受渡し方法に係わり、特に高度なセキュリティを確保するファイル共有システム、プログラムおよび共有ファイル受渡し方法に関する。

【０００２】

【従来の技術】複数のクライアント端末がお互いにネットワークを利用してデータを共有する場合、例えばＮＦＳ（Network File System）やＷＥＢ等の技術が利用されている。

【０００３】このＮＦＳにおいては、各クライアント端末がネットワークを経由してディスクを共有するＵＮＩＸ（登録商標）マシンで最も普及している分散ファイルシステムであって、各ユーザがファイルサーバのファイルの利用に際し、クライアント端末から入力されるユーザ名・パスワード等の認証情報をファイルサーバのＯＳが認証することを前提とし、ファイルサーバに付設されているディスクが離れたところから見える状態となり、必要なファイルを利用することが可能となる。

【０００４】一方、ＷＥＢの技術を利用したシステムは、ネットワークに接続されるクライアント端末がＷＥＢページを提供するサーバに対してＵＲＬ（Uniform Resource Locater）のもとにアクセスし、必要なファイルのＨＴＭＬ言語を解読し表示するネットワークシステムであり、専らファイルを参照することが目的となる。

【０００５】このようなクライアント／サーバ・システムでは、ファイルサーバ上に保存されているファイルを

参照する場合、各クライアント端末がサーバにログインしたり、共有するファイル格納領域をアクセスすることにより、サーバ上のファイルを参照する。

【０００６】

【発明が解決しようとする課題】従って、以上のようなシステムでは、ファイルサーバがアクセス制御情報を管理し、各クライアント端末からの認証情報に対し、ファイルサーバのＯＳで管理されているアクセス制御情報に基づき、ファイルのアクセス可否を決定している。よって、ファイルサーバのＯＳによりファイルの参照権、更新権等を設定することによってアクセス方法を制御することが可能であるが、この設定された参照権により、ファイル名称を格納するディレクトリ内に保存される参照不可能なファイルのファイル名称も参照可能となる。

【０００７】よって、現状のシステムのファイル共有では、ファイルサーバのアクセス制御に依存しているので、参照権の無いファイルでも、参照権のあるディレクトリ内に保存されている参照不可能なファイルのファイル名称も参照可能となるので、例えばディレクトリ内からファイル名称の格納場所を読み取ることが可能となり、参照不可能なファイルの参照やファイルの改竄等が行われる可能性がある。

【０００８】本来、セキュリティを重要視するシステムでは、ファイルの存在すらも参照されてはならない場合が存在するが、ファイルサーバのＯＳで管理されるアクセス制御に依存することから、セキュリティの確保が非常に難しい。

【０００９】本発明は上記事情にかんがみてなされたもので、ファイルサーバからファイルのアクセス制御に関する情報を独立させ、柔軟なアクセス制御を実現するファイル共有システム、プログラムおよび共有ファイル受渡し方法を提供することを目的とする。

【００１０】また、本発明の他の目的は、厳密なセキュリティを確保するファイル共有システム、プログラムおよび共有ファイル受渡し方法を提供することにある。

【００１１】

【課題を解決するための手段】（１）　上記課題を解決するために、複数の端末がネットワークを利用してファイルを共有する本発明に係わるファイル共有システムは、ファイルを格納する少なくとも１台のファイルサーバと、このファイルサーバから独立して前記ファイルのアクセス制御情報を管理し、前記端末からのアクセス要求に基づいて当該アクセス制御情報を参照し、要求権限に応じて前記ファイルサーバからファイルを取得し要求元端末に転送するアクセス制御サーバとを備えた構成である。

【００１２】本発明は、以上のような構成とすることにより、各端末とファイルサーバとの間にファイルのアクセス制御情報を管理するアクセス制御サーバを設けたことにより、端末からのアクセス要求に対し、アクセス制御サーバがアクセス制御情報を参照し、アクセス要求に応じた権限を有するか否かを判断し、権限を有する場合には必要に応じてファイルサーバからファイルを取得し、要求元端末に転送するので、柔軟なアクセス制御を実現することが可能である。

【００１３】（２）　本発明に係わる共有ファイルシステムは、ファイルを共有する複数の端末と、ファイルを格納する少なくとも１台のファイルサーバと、ファイルのアクセス制御情報を管理し、複数の端末と少なくとも１台のファイルサーバとに対して、異なるネットワークで接続されているアクセス制御サーバとを設けた構成である。

【００１４】本発明は、以上のような構成とすることにより、アクセス制御サーバと端末およびファイルサーバとが異なるネットワークで接続され、かつ、アクセス制御サーバがファイルのアクセス制御情報を管理することにより、厳密な意味でのセキュリティを確保することが可能である。

【００１５】（３）　本発明に係わるプログラムは、各端末からのファイルのアクセス要求を受け、ファイルサーバに格納されるファイルを要求し前記要求元端末に転送するコンピュータに、各端末から送信されてくるファイルのアクセス要求フォーマットに記載するファイル名およびユーザに関連する識別データに基づき、予め管理されているアクセス制御情報を参照し、ファイル名に相当する論理ファイル、前記識別データと同一の識別データが存在するか否かを判断するファイル・ユーザ存在検索機能と、この機能によって存在すると判断されたとき、アクセス要求フォーマットに記載する要求種別を判断する要求種別判断機能と、この機能によって判断された要求種別がアクセス制御情報に定める権限に合致するか否かを判断する権限チェック機能と、この機能により権限有りと認定されたとき、ファイルサーバと連携し要求種別を実行する機能とを実現させるものである。

【００１６】本発明は、以上のような構成とすることにより、コンピュータに以上のような諸機能を実現させるプログラムを有することにより、各端末からファイルのアクセス要求フォーマットを受けたとき、コンピュータでは、アクセス要求フォーマットに記載される情報に基づき、アクセス制御情報を参照し、ファイルの存在および予め登録されているユーザかを検索し、何れも存在有りのとき、アクセス要求フォーマットに記載する要求種別を判断し、さらにユーザが要求種別に対する権限をもっているかを判断し、権限有りと認定されたとき、要求種別に応じてファイルサーバからファイルを取得し要求元端末に転送するので、アクセス制御情報の定義いかんにより、柔軟なアクセス制御および高度なセキュリティを確保しつつファイルサーバの実体的なファイルを転送することが可能である。

【００１７】（４）　本発明に係わる共有ファイル受渡

し方法は、各端末から所定のアクセス要求フォーマットに応じたアクセス要求を送出するアクセス要求ステップと、ファイルのアクセス制御情報を管理するアクセス制御サーバが各端末から送信されてくるファイルのアクセス要求フォーマットに記載されるファイル名およびユーザに関連する識別データに基づき、アクセス制御情報を参照し、ファイル名に相当する論理ファイル、識別データと同一の識別データが存在するか否かを検索する検索ステップと、このステップにより存在すると判断されたとき、前記アクセス制御サーバがアクセス要求フォーマットに記載する要求種別を判断する要求種別判断ステップと、このステップにより判断された要求種別に基づき、前記アクセス制御サーバがアクセス制御情報を参照し、当該要求種別に対する権限有無をチェックする権限チェックステップと、このステップによって権限有りと判断されたとき、前記アクセス制御サーバが前記要求種別に応じてファイルリストを前記要求元端末に転送し、或いは前記ファイルサーバにファイルを要求し、取得されたファイルを前記要求元端末に転送する転送ステップとを有するので、要求種別に応じてファイルサーバからファイルを取得し要求元端末に転送するので、柔軟なアクセス制御の実現、高度なセキュリティを確保しつつファイルサーバの実体的なファイルを要求元端末に渡すことが可能となる。

【００１８】

【発明の実施の形態】以下、本発明に係わるファイル共有システムの一実施の形態について図１を参照して説明する。

【００１９】このファイル共有システムは、ファイルに対して所要のアクセス要求を行う複数台のクライアント端末１，…と、これらクライアント端末１，…からのアクセス要求種別に応じて必要なファイルの転送・非転送その他の処理を実行するアクセス制御サーバ２と、実体的なファイルが格納されている少なくとも１台のファイルサーバ３とによって構成されている。アクセス制御サーバ２は、各クライアント端末１，…およびファイルサーバ３に対してそれぞれ異なるネットワーク４、５で接続することにより、クライアント端末１からファイルサーバ３に直接にアクセスできないゲートウェイとしての役割をもっている。よって、クライアント端末１の認証情報の他、端末１とアクセス制御サーバ２との間のネットワークは十分に信頼できる環境に確保されているものである。

【００２０】クライアント端末１は、アクセス制御サーバ２に所要のアクセス要求を行うためのファイル参照用アプリケーション１１、このアプリケーション１１などからのアクセス要求を受け付けるためのインタフェースを有し、このインタフェースにより受け付けたアクセス要求の情報に対して所要のアクセス方法や経路などの制御を実行するアクセス制御層１２およびこのアクセス制御層１２を通ってくる所定のアクセス要求フォーマットのアクセス要求情報をアクセス制御サーバ２に転送するネットワーク層１３が設けられている。

【００２１】このアクセス要求フォーマットは、図２に示すごとく例えばユーザ識別ＩＤ、グループ識別ＩＤ、端末名、アクセス対象となるファイル名、ファイルの要求種別、参照条件等の項目名が挙げられる。ユーザ識別ＩＤはユーザが本人であることを識別させるユーザ名やパスワード等であって、ＯＳの認証情報となる。グループ識別ＩＤは、同じ条件・価値を有する複数人のユーザのグループを識別させるグループ名やパスワード等であって、同様にＯＳの認証情報となる。要求種別としては、例えばファイル名の一覧、対象ファイルの取得、対象ファイルへの書込みを行う更新、削除などである。参照条件はファイルリストを取得するための参照条件である。

【００２２】アクセス制御サーバ２は、実体のファイルが格納されている領域を共有せずにクライアント端末１からの要求に応じて必要なファイルのみを転送・非転送を実行する機能を有するものであって、ファイルサーバ３のＯＳから独立してファイルのアクセス制御情報２１を管理し、ファイルの格納より柔軟なアクセス制御を実現する。

【００２３】すなわち、アクセス制御サーバ２は、システム内で取り扱っているファイルのアクセス情報２１を含む管理情報を一元的に管理する一方、アクセス制御層２２、ファイル代理転送部２３および異なるネットワーク４，５に対して所定の通信規則に従ってデータの授受を行うネットワーク対応のネットワーク層２４，２５が設けられている。

【００２４】前記アクセス制御層２２は、端末１から受信した所定フォーマットのアクセス要求情報とアクセス制御サーバ２で管理するアクセス制御情報２１とを照合し、端末１からのアクセス要求種別の可否を判定するアクセス制御機能をもっている。このアクセス制御サーバ２が管理するアクセス制御情報２１のフォーマットは、図３に示すように例えば論理ファイル名、論理ディレクトリ名、ファイルの作成日時、ファイルの更新日時、ファイルサーバのホスト名であるファイルサーバ名、ファイルサーバ上の物理的ファイル名、ファイルサーバ上の物理的ディレクトリ名、ファイル作成者であるオーナ名、アクセス情報の種別を表すアクセスタイプ、ユーザ識別ＩＤ，グループ識別ＩＤ，端末識別その他のアクセス情報、ｒｗｄｘｃ（ｒ：リード、ｗ：ライト，ｄ：デリート，ｘ：実行，ｃ：更新）などの権限などが挙げられる。

【００２５】前記ファイル代理転送部２３は、アクセス制御層２２でのクセス要求可否の判定結果、ファイルへのアクセスが許可された場合、図２に示すアクセス要求フォーマットのアクセス要求情報として記述されている

ファイル名からファイルが保存されているファイルサーバ３のホスト名、格納先の物理ディレクトリ、物理ファイル名に変換し、ファイルサーバ３にファイル転送を要求し、ファイルサーバ３に代わって要求元クライアント端末１に該当ファイルを転送する機能をもっている。なお、ファイル代理転送部２３は、アクセス制御層２２においてファイルへのアクセスが許可されない場合、端末１に対してアクセスが拒否された旨のステータスを戻す一方、ファイルサーバ３におけるディスク上のログファイルにアクセス情報を保存し、後に管理者が容易に見られる状態に設定する。

【００２６】前記ファイルサーバ３は、実際上、複数台のファイルサーバからなり、それぞれ例えばディスク上に保存される実体としてのファイル３１、このファイル３１を読み出して転送するファイル転送サーバ３２、アクセス制御層３３およびネットワーク層３４によって構成されている。

【００２７】従って、以上のようなファイル共有システムの実施の形態によれば、ファイルのアクセス制御情報を管理するアクセス制御サーバ２を設け、端末１からのアクセス要求に対し、アクセス制御サーバ２がアクセス制御情報を参照し、アクセス要求に応じた権限を有するとき、その権限内にファイルサーバ３からファイルを取得し、要求元端末１に転送するので、アクセス制御情報に記述する定義内容に応じて柔軟なアクセス制御を実現することができる。

【００２８】また、アクセス制御サーバ２と端末１およびファイルサーバ３が異なるネットワーク４，５で接続され、かつ、アクセス制御サーバ２がファイルのアクセス制御情報を管理することにより、端末１から直接ファイルサーバ３をアクセスできず、しかも端末１からのアクセス要求に対してアクセス制御サーバ２が権限のチェックを行い、権限内において必要に応じてファイルサーバ３にファイルを要求し、要求元端末に転送するので、厳密なセキュリティを確保することが可能である。

【００２９】次に、以上のようなシステムを用いて本発明に係わる共有ファイル受渡し方法作およびプログラムの一連の処理例について図４を参照して説明する。

【００３０】クライアント端末１は例えば自身のユーザ識別ＩＤまたはグループ識別ＩＤ、処理対象となるファイル名、ある１つの要求種別および参照条件等の指定のもとに図２に示す所定フォーマットのアクセス要求情報をイーサネット（登録商標）（商標名）などのネットワーク４上に送信する（アクセス要求ステップ）。

【００３１】コンピュータであるアクセス制御サーバ２のネットワーク層２４がアクセス要求情報を受信し、アクセス制御層２２に渡す。このアクセス制御層２２は、アクセス要求情報有りか否かを判断し（Ｓ１）、当該情報有りと判断したとき、その情報の中のファイル名およびユーザ識別ＩＤまたはグループ識別ＩＤに基づき、図３に示すアクセス制御情報フォーマットに論理ファイル名およびオーナ名を検索し、ファイル名に相当する論理ファイル名が登録されているか、またオーナ名には要求元ユーザ識別ＩＤまたはグループ識別ＩＤと同一のユーザ識別ＩＤまたはグループ識別ＩＤが登録されているか否かを検索する（Ｓ２、Ｓ３：ファイル・ユーザ存在検索機能、検索ステップ）。

【００３２】引き続き、要求種別に伴う要求元であるユーザの権限をチェックする。この権限チェックは、アクセス要求情報の要求種別が一覧，取得、更新、その他の何れかであるかを判断する（Ｓ４～Ｓ６：要求種別判断機能、要求種別判断ステップ）。

【００３３】ここで、アクセス要求情報の要求種別からファイルリスト一覧要求と判断すると、アクセス要求フォーマットに指定されているる参照条件がアクセス制御情報フォーマットの権限に合致するか否かを判断し（Ｓ４１：一覧権限チェック機能、権限チェックステップ）、合致する場合には要求元ユーザ識別ＩＤまたはグループ識別ＩＤで許可された論理ファイル名（ファイルリスト）を要求元であるクライアント端末１に転送する（Ｓ４２：ファイルリスト一覧転送機能、転送ステップ）。従って、アクセスが許可されたファイル以外の情報が端末１に転送されることはない。

【００３４】次に、アクセス要求情報に記述される要求種別がファイル取得と判断されたとき、前述する論理ファイル名のアクセス権限がアクセス制御情報フォーマットの中の「権限」内で認定されているか否かを判断し（Ｓ５１：取得権限チェック機能、権限チェックステップ）、論理ファイル名に対するアクセス権限が認定されている場合には、当該論理ファイル名に対応するファイルサーバ名、物理ファイル名を検索し、ファイル代理転送部２３がファイルサーバ３上のファイル転送サーバ３２に対して物理ファイルを要求し、ファイル転送サーバ３２から物理ファイルを取得する（Ｓ５２：物理ファイル要求取得機能）。しかる後、この取得されたファイルを論理ファイル名に変換し（Ｓ５３：ファイル名変換機能）、この論理ファイル名をもったファイルを要求元端末１に転送する（Ｓ５４：ファイル転送機能、転送ステップ）。

【００３５】さらに、ステップＳ６において、アクセス要求情報の要求種別がファイル更新と判断されたとき、前述する論理ファイル名のアクセス権限がアクセス制御情報フォーマットの中の「権限」内で認定されているか否かを判断し（Ｓ６１：更新権限チェック機能、権限チェックステップ）、論理ファイル名に対するアクセス権限が認定されている場合には、当該論理ファイル名に対応するファイルサーバ名、物理ファイル名を検索し、ファイル代理転送部２３がファイルサーバ３上のファイル転送サーバ３２に対して物理ファイルを要求し、ファイル転送サーバ３２から物理ファイルを取得する（Ｓ６

２：物理ファイル要求取得機能）。しかる後、この取得されたファイルを論理ファイル名に変換し（Ｓ６３：ファイル名変換機能）、この論理ファイル名をもったファイルを要求元端末１に転送する（Ｓ６４：ファイル転送機能、転送ステップ）。

【００３６】しかる後、アクセス制御サーバ２が端末１から更新されたファイルを受け取ると、ファイル代理転送部２３がファイルサーバ３上のファイル転送サーバ３２に対して物理ファイル名のもとに適切なファイルサーバ３に対して更新ファイルの登録を要請する（Ｓ６５）。適切なファイルサーバとは、サーバの空き容量、負荷状態、秘密のレベル等の情報によって選択されるファイルサーバを意味する。

【００３７】よって、要求元端末１からは実際のファイルがどのファイルサーバ３に格納されているかを意識することなく、ファイルの更新が可能となる。

【００３８】なお、各端末からのアクセス要求に対し、アクセス制御サーバ２がアクセス要求を不許可とした場合には、その要求元端末１に対してアクセスが拒否された旨のステータスを戻す一方、ファイルサーバ３のディスク上のログファイルにアクセス情報を保存する（Ｓ７０）。

【００３９】従って、以上のような実施の形態によれば、各端末からファイルのアクセス要求フォーマットを受けたとき、コンピュータでは、予め定めるプログラムに従い、アクセス要求フォーマットに記載される情報に基づき、アクセス制御情報を参照し、該当ファイル名の存在および予め共有ユーザとして登録されているかを検索し、何れも有りと判断されたとき、ユーザの要求種別に対する権限をもっているかを判断し、権限有りと認定されたとき、要求種別に応じてファイルサーバ３からファイルを取得し要求元端末に転送するので、柔軟なアクセス制御の実現の他、高度なセキュリティを確保しつつファイルサーバ３の実体的なファイルを転送できる。

【００４０】さらに、以上のような共有ファイルの受渡し方法によれば、端末の要求種別に対する権限をチェックし、例えばファイル取得，ファイル更新の権限有り場合には、ファイルサーバ３からファイルを取得し要求元端末に転送するので、高度なセキュリティを確保しつつファイルサーバ３の実体的なファイルを要求元端末に渡したり、更新したファイルをファイルサーバ３に転送し登録することができる。

【００４１】その他、本願発明は、上記実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々変形して実施できる。また、各実施の形態は可能な限り組み合わせて実施することが可能であり、その場合には組み合わせによる効果が得られる。さらに、上記各実施の形態には種々の上位，下位段階の発明が含まれており、開示された複数の構成要素の適宜な組み合わせにより種々の発明が抽出され得るものである。例えば問題点を解決するための手段に記載される全構成要件から幾つかの構成要件が省略されうることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【００４２】

【発明の効果】以上説明したように本発明によれば、ファイルサーバからファイルのアクセス制御に関する情報を独立させることにより、アクセス制御情報に規定する定義に応じて柔軟なアクセス制御を実現できるファイル共有システム、プログラムおよび共有ファイル受渡し方法を提供できる。

【００４３】また、本発明の他の目的は、端末のアクセス要求に対し、端末からファイルサーバに対して直接アクセスさせずに、アクセス制御サーバがアクセス制御情報を管理し、要求内容を判断し権限をチェックし、ファイルサーバのファイルを要求し、要求端末に転送するので、、厳密にセキュリティを確保できるファイル共有システム、プログラムおよび共有ファイル受渡し方法を提供できる。

【図面の簡単な説明】

【図１】　本発明に係わるファイル共有システムの一実施形態を示す構成図。

【図２】　図１に示す端末から出力される所定フォーマットのアクセス要求情報の配列例図。

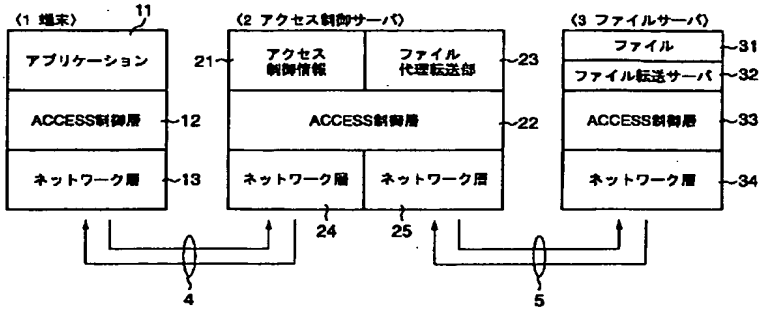
【図３】　図１に示すアクセス制御サーバが管理するアクセス制御情報フォーマット図。

【図４】　本発明に係わるプログラムの処理例および共有ファイル受渡し方法を説明するフローチャート。

【符号の説明】

１…クライアント端末
２…アクセス制御サーバ
３…ファイルサーバ
４，５…異なるネットワーク
１１…ファイル参照用アプリケーション
２１…アクセス制御情報
２２…アクセス制御層
２３…ファイル代理転送部
３１…実体のファイル
３２…ファイル転送サーバ

【図１】



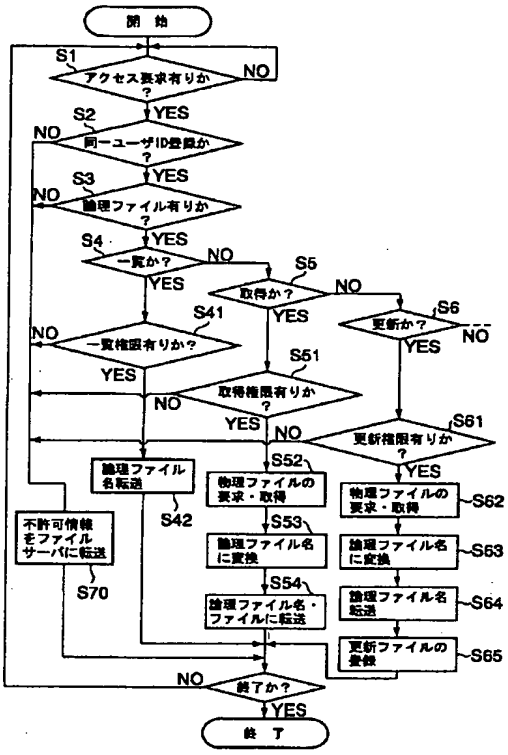
【図２】

項目名	概要
ユーザ識別ID	OSの認証情報
グループ識別ID	OSの認証情報
端末名	端末の情報
ファイル名	アクセス対象のファイル名
要求種別	一覧, 取得, 更新, 削除
参照条件	ファイルリスト取得のための参照条件

【図３】

項目名	概要
論理ファイル名	論理的なファイル名
論理ディレクトリ名	論理的なディレクトリ名
作成日時	ファイルの作成日時
更新日時	ファイルの更新日時
ファイルサーバ名	ファイルサーバのホスト名
物理ファイル名	ファイルサーバ上の物理的なファイル名
物理ディレクトリ名	ファイルサーバ上の物理的なディレクトリ名
オーナー名	ファイルのオーナー名（ユーザ識別ID）
アクセスタイプ	アクセス情報の種別を表す。 1:ユーザ 2：グループ 3：端末 4:その他
アクセス情報	ユーザ識別ID, グループ識別ID, 端末識別コード, その他
権限	rwdxc

【図４】



フロントページの続き

Ｆターム(参考) 5B017 AA01 BA06 BB06 CA16
5B082 EA11 HA05 HA08
5B085 AA01 AE01 BA07 BG03 BG07